UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−013

Vulnerabilidad en el generador de números aleatorios de OpenSSL en Debian/Ubuntu

---

Una vulnerabilidad en el paquete OpenSSL incluido en los sistemas Debian GNU/Linux y sus derivados puede causar que se generen llaves criptográficas débiles. Cualquier paquete que utilice la versión de SSL afectada, podría ser vulnerable.

Fecha de Liberación: 19 de Mayo de 2008

Ultima Revisión: 19 de Mayo de 2008

Fuente:

Riesgo

Crítico

Problema de Vulnerabilidad

Local y remoto

I. Sistemas Afectados

- Debian, Ubuntu y Sistemas basados en Debian

II. Descripción

Existe una vulnerabilidad en el generador de números aleatorios utilizado por el paquete OpenSSL incluido en Debian GNU / Linux, Ubuntu y otros sistemas basados en Debian. Esta vulnerabilidad hace que el número generado pueda ser previsible.

El resultado de este error es que algunas claves de cifrado son más comunes de lo que debieran ser. Esta vulnerabilidad afecta a todas las aplicaciones que utilizan claves generadas con la versión afectada del paquete OpenSSL. Las llaves que pueden ser afectadas, sin que se limiten a las mismas, son las llaves de SSH, OpenVPN, DNSSEC y las llaves generadas para el usos de certificados en formato X.509 y las llaves de sesión utilizadas para conexiones SSL/TLS. Cualquier llave generada en o después del 17 de septiembre de 2006 pueden ser vulnerables. Las claves generadas con GnuPG, GNUTLS, ccrypt u otras aplicaciones de cifrado que no utilicen OpenSSL no son vulnerables debido a

que utilizan sus propios generadores de número aleatorios.

III. Impacto

Un intruso, de forma remota y sin necesidad de autenticarse, podría adivinar la clave secreta. De igual forma, un intruso podría explotar esta vulnerabilidad para acceder al equipo afectado de forma no autorizada a través del sevicio afectado o hacer un ataque de “hombre en medio”.

IV. Solución

Actualización

Debian y Ubuntu han publicado versiones corregidas de OpenSSL que reparan dicho problema. Los administradores podrán utilizar la aplicación ssh−vulnkey para checar si sus claves son vulnerables. Después de aplicar la actualización, es probable que los clientes no puedan conectarse a los servidores.

Solución temporal

Durante el período de tiempo en el que no se aplique la actualización, se deben tomar medidas para restringir el acceso a los servidores o equipos afectados. Para dicho fin, los sistemas basados en Debian y Ubuntu, pueden utilizar iptables o tcp−wrappers.

V. Referencias

- DSA−1571−1 openssl −− predictable random number generator − <http://www.debian.org/security/2008/dsa−1571>
- Debian wiki − SSL keys − <http://wiki.debian.org/SSLkeys>
- Ubuntu OpenSSL vulnerability − <http://www.ubuntu.com/usn/usn−612−1>
- Ubuntu OpenSSH vulnerability − <http://www.ubuntu.com/usn/usn−612−2>
- Ubuntu OpenVPN vulnerability − <http://www.ubuntu.com/usn/usn−612−3>
- Ubuntu SSL−cert vulnerability − <http://www.ubuntu.com/usn/usn−612−4>
- Ubuntu OpenSSH update − <http://www.ubuntu.com/usn/usn−612−5>
- Ubuntu OpenVPN regression − <http://www.ubuntu.com/usn/usn−612−6>
- OpenVPN regression − <http://www.ubuntu.com/usn/usn−612−6>
- Vulnerability Note VU#925211 − <http://www.kb.cert.org/vuls/id/925211>

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Israel Becerril Sierra (ibecerril at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

---

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47